

Claims

- 5 1. Apparatus for use in transactions, comprising:
non-volatile memory containing a set of multiple identifiers associated with a customer account,
wherein said multiple identifiers are also known to an agency providing said customer account, and
a processor operable to select one identifier from said set of multiple identifiers for use with any
transaction involving said customer account.
- 10 2. The apparatus of claim 1, wherein each of the identifiers in said set of multiple identifiers is
allocated by the agency uniquely to the apparatus.
- 15 3. The apparatus of claim 1, further comprising a communications facility to engage a terminal,
wherein the apparatus is operable to receive bill details for a transaction from the terminal, to generate a
transaction record from the bill details, and to transmit the transaction record to the terminal.
- 20 4. The apparatus of claim 3, wherein the transaction record includes a digital signature that is
generated using a cryptographic key contained within the non-volatile memory.
- 25 5. The apparatus of claim 3, wherein the transaction record is encrypted.
6. The apparatus of claim 1, wherein said apparatus is provided within inert packaging to allow
implantation into the human body.
- 30 7. The apparatus of claim 1, wherein said apparatus is operable to engage a first class of terminals for
making a transaction, and a second class of terminals to enter or to update account information stored in the
non-volatile memory.
8. The apparatus of claim 7, further comprising first and second power circuits that are activated by
said first and second class of terminals respectively, wherein activation of said second power circuit does
not allow account information to be entered or updated in at least certain portions of said non-volatile
memory.
- 35 9. A method for making a transaction with a device, comprising:
storing within the device a set of multiple identifiers associated with a customer account, wherein
said multiple identifiers are also known to an agency providing said customer account, and

selecting one identifier from said set of multiple identifiers for use with a transaction involving said customer account.

10. The method of claim 9, wherein each of the identifiers in said set of multiple identifiers is
5 allocated by the agency uniquely to the device.

11. The method of claim 9, wherein making a transaction further comprises:
engaging a terminal,
receiving bill details for a transaction from the terminal,
10 generating a transaction record from the bill details, and
transmitting the transaction record to the terminal.

12. The method of claim 11, wherein the transaction record includes a digital signature that is
generated using a cryptographic key contained within the non-volatile memory.
15

13. The method of claim 11, further comprising encrypting the transaction record.

14. The method of claim 9, further comprising limiting the transaction rate of the device to prevent
rapid read-out of the identifiers.
20

15. Apparatus for use in transactions, including:
means for storing a set of multiple identifiers associated with a customer account, wherein said
multiple identifiers are also known to an agency providing said customer account, and
means for selecting one identifier from said set of multiple identifiers for use with any transaction
25 involving said customer account.

16. Apparatus for use in making a transaction, including:
non-volatile memory containing a set of multiple identifiers, wherein said multiple identifiers are
also known to an agency associated with the transaction, and
30 a processor operable to select one identifier from said set of multiple identifiers for use in any
transaction.

17. A method for opening an account on a portable transaction device comprising:
opening an account record in an agency computer system, wherein said agency is to provide the
35 account,
generating a set of multiple identifiers to be used for transactions on the account,
storing the set of multiple identifiers in the agency computer system, and

storing the set of multiple identifiers on the portable transaction device.

18. The method of claim 17, wherein the identifiers are unique to the account for the agency.

5 19. The method of claim 18, further comprising adding the identifiers to an index, wherein said index maps from an identifier to the corresponding account.

20. The method of claim 17, wherein the identifiers are sparsely distributed across the set of possible identifiers.

10

21. The method of claim 17, wherein the identifiers within said set of multiple identifiers are unrelated to one another.

15

22. The method of claim 17, wherein the identifiers are generated on the agency computer system, and are transmitted to the portable transaction device for storage thereon.

23. The method of claim 17, further comprising generating at least one cryptographic key for use with the account.

20

24. The method of claim 17, further comprising making a prepayment onto the account prior to using the account for transactions.

25. The method of claim 17, further comprising establishing an identity of a person who is to hold the account prior to opening the account.

25

26. A method for performing a transaction at a terminal using a portable transaction device, comprising:

30

generating a bill for the transaction at the terminal,

engaging the portable transaction device with the terminal,

transmitting the bill from the terminal to the transaction device,

selecting one identifier from a set of multiple identifiers stored on the transaction device for use in the transaction,

generating a transaction record on the transaction device, the transaction record incorporating information from the bill and the selected identifier, and

35

transmitting the transaction record to the terminal.

27. The method of claim 26, wherein the transaction record includes a digital signature from the transaction device.
28. The method of claim 26, wherein the transaction device is associated with a customer account, and wherein said multiple identifiers are also known to an agency providing said customer account, the method further comprising:
- transmitting the transaction record from the terminal to an agency computer,
 - accessing an account record for the customer account based on the selected identifier included in the transaction record,
 - validating the transaction, and
 - updating the account record in respect of the validated transaction.
29. The method of claim 28, wherein prior to transmitting the transaction record from the terminal to the agency computer, the terminal incorporates its own copy of the bill into the transaction record.
30. A method of operating a computer account system at an agency, said agency maintaining a plurality of customer accounts on the computer account system, wherein each customer account has a set of multiple identifiers associated therewith, the method comprising:
- receiving a request for a transaction on a customer account,
 - accessing an identifier within the request,
 - determining which set of multiple identifiers the accessed identifier belongs to, and from this determining a customer account for the transaction, and
 - updating the determined customer account in respect of the transaction.
31. The method of claim 30, wherein determining which set of multiple identifiers the accessed identifier belongs to comprises accessing an index that maps identifiers to corresponding account records.
32. The method of claim 30, wherein the request includes a digital signature generated by a transaction device associated with a customer account, and the method further comprises validating the digital signature.
33. The method of claim 30, further comprising opening a new customer account by:
- creating a new account record for the new customer account, and
 - storing a set of multiple identifiers associated with the new customer account into the new account record.
34. The method of claim 33, further comprising:

generating the set of multiple identifiers associated with the new customer account, and
transmitting the generated set of multiple identifiers to a customer transaction device for use with
the new customer account.

5 35. The method of claim 33, further comprising generating at least one cryptographic key for use in
communications between the computer account system and the customer transaction device.

36. A computer account system at an agency, said system comprising:
a plurality of customer account records, wherein each customer account record incorporates a set
10 of multiple identifiers associated therewith, and
an index that maps identifiers to corresponding account records,
wherein the system is responsive to receiving a request for a transaction on a customer account to
access an identifier within the request in order to determine which set of multiple identifiers and hence
which customer account the accessed identifier belongs to.

15 37. The system of claim 36, wherein the multiple identifiers associated with a customer account
record are unique to that account record.

38. The system of claim 36, wherein each account record also includes a cryptographic key for use in
20 validating a digital signature for transaction records associated with that account.

39. A computer account system at an agency, said system comprising:
Means for storing a plurality of customer account records, wherein each customer account record
incorporates a set of multiple identifiers associated therewith,
25 Means for mapping identifiers to corresponding account records,
Means for accessing an identifier within a received transaction request to determine which set of
multiple identifiers and hence which customer account the accessed identifier belongs to, and
Means for updating the customer account to which the accessed identifier belongs in accordance
with the received transaction request.

30